

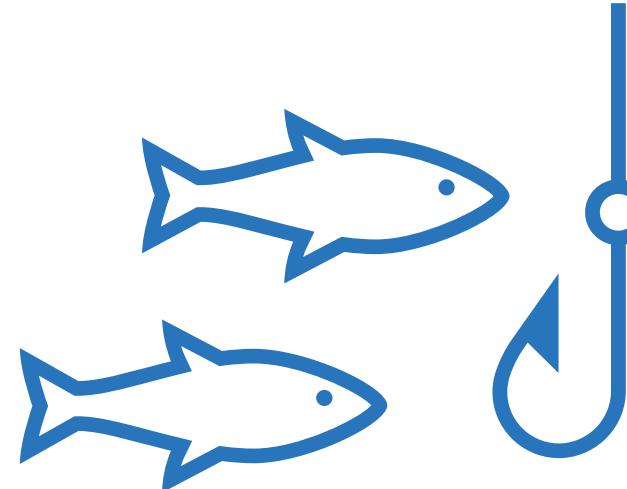
Kako prepoznati kibernetičke prijetnje i zaštитiti se?

CARNET – Odjel za Nacionalni CERT

Sadržaj

1. Vrste računalno-sigurnosnih ugroza
2. Prepoznavanje
3. Zaštita
4. Prijava
5. Vježbe

- Phishing
- Poslovna prijevara
- Ransomware
- Iznuda
- Scam
- Spam



- Pokušaj navođenja pojedinca na odavanje povjerljivih podataka ili pokretanje zlonamjernog programa, putem e-pošte
 - sms (*smishing*)
 - poziv (*vishing*)
 - *Whaling* = cilja osobu na rukovodećoj poziciji (npr. ravnatelja)
 - *Spearphishing* = cilja točno određenu žrtvu o kojoj unaprijed istraži informacije (npr. ravnatelja, tajnicu)
 - *Catphishing* = napadač stvara lažni identitet, ulazi u komunikaciju sa žrtvom, u svrhu dobivanja povjerljivih informacija
-

Šalje: E-dnevnik Potvrde <e.dnevnik.potvrde@gmail.com>

Poslano: 13. siječnja 2022. 20:34

Prima:

Predmet: E-dnevnik Potvrde

Poštovani profesori,

Radi osvježavanja sustava i ažuriranja došlo je do gubljenja podataka.

Molimo vas da što prije potvrdite vaš CARNET mail [OVDJE](#).

Hvala!



<http://e-dnevnik-potvrde.c1.biz/>

e-Dnevnik

E-pošta

Lozinka

From [Mreza-oam] [CN Mreza] <mreza@carnet.hr> <agm_sales@azizgroupbd.com>

To d...ja@carnet.hr

Subject Fwd: d..._a@carnet.hr

Hi

Please see attachment for your scanned document

MAIL_0902.zip

ARCHIVE PASS - 6607

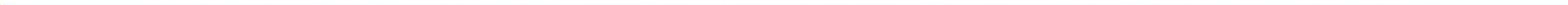
Mreza-oam

mreza-oam-bounces@carnet.hr

▼ 1 Attachment 14,5 KB

 MAIL_0902.zip 14,5 KB

- napadač lažnim predstavljanjem pokušava steći ili stekne financijsku korist od ciljanog poslovnog korisnika (npr. računovodstvo, kadrovska i sl.)
- BEC (eng. *business email compromise*) prijevara
 - Napadač ulazi u komunikaciju između dva djelatnika
 - Predstavlja se kao osoba na rukovodećoj poziciji ili dobavljač
 - Traži hitno plaćanje računa
 - Preusmjerava račun u svoju korist



From Dobavljac <dobavljac@tvrtka.hr>

To a@carnet.hr

Subject Zahtjev za nabavom - Narudžbenica 22022022

Dobro jutro,

U prilogu je lista narudžbi proizvoda za vašu referencu.

Kupac nam je poslao vašu kontakt email adresu: nabava@carnet.hr

Priložio sam skeniranu kopiju proizvoda koji su nam potrebni i njihove potrebne specifikacije jedinica.

Pošaljite mi ponudu sa vašim najboljim cijenama, dostupnošću i mogućim opcijama dostave.

Radujemo se vašem blagovremenom odgovoru.

Srdačan pozdrav,

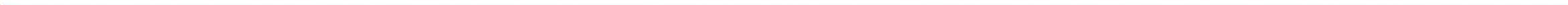
--

Pero Perić
Glavni računovođa
Tvrtka d.o.o
Ulica broj 12, Split
tel: +385 1 1234 567
www.tvrtka.hr

- Napadač lažira polje pošiljatelja da izgleda kao da je e-pošta poslana s legitimne adrese ili kompromitira stvarni korisnički račun e-pošte
 - Cilja kadrovsku ili računovodstvo
 - Predstavlja se kao osoba na rukovodećoj poziciji (CEO, ravnatelj)
 - Traži prijenos novca ili povjerljive informacije
 - Traži hitnu reakciju



- vrsta zlonamjernog programa kojem je cilj šifriranje računalnog sustava ili datoteka žrtve i traženje otkupnine
 - Traži hitnu reakciju (vremenski rok za plaćanje otkupnine)
 - Prenosi se elektroničkom poštom, putem web stranica ili fizičkog uređaja
 - Za poznate vrste ransomwarea postoje ključevi za dešifriranje
 - <https://www.nomoreransom.org/crypto-sheriff.php?lang=cro>





- pokušaj navođenja pojedinca na plaćanje iznude, najčešće lažnim informacijama i zastrašivanjem
 - npr. *sextortion*



Pozdrav!

Nažalost, imam neke loše vijesti za vas.

Prije otprilike nekoliko mjeseci dobio sam pristup vašim uređajima kojima ste se koristili za pregledavanje interneta.

Nakon toga nastavio sam s praćenjem vaših internetskih aktivnosti.

U nastavku slijedi niz prošlih dogadaja:

U prošlosti sam od hakera kupio pristup brojnim računima e -pošte (danas je to vrlo jednostavan zadatak koji se može obaviti online).

Naravno, bez napora sam se prijavio na vaš račun e -pošte ().

Riješimo to ovako:

Trebate samo prebaciti 9000 Kn na moj račun (ekvivalent bitcoina na temelju tečaja tijekom vašeg prijenosa),
a nakon što transakcija bude uspješna, bez odlaganja ću izbrisati sve te perverzne stvari.

Poslije se možemo pretvarati da se nikad nismo sreli.

Osim toga, uvjeravam vas da će sav štetni softver biti izbrisani sa svih vaših uređaja. Budite sigurni, ja držim svoja obećanja.

Dobit ćete najviše 48 sati nakon što otvorite ovu e-poruku (točnije, 2 dana).

- pokušaj vještog navođenja potencijalne žrtve na djelovanje u korist prevaranta
 - npr. nigerijski princ / romantična prijevara / brza zarada / humanitarna akcija

Pažnja: korisnik sredstava,

Poslao sam vam ovo pismo prije mjesec dana, ali nisam se javio, nisam siguran da li ste ga dobili, i zato ga ponavljam. Prvo, ja sam gđa Kristalina Georgieva, generalni direktor i Predsjednica Međunarodnog monetarnog fonda.

Doista, pregledali smo sve prepreke i probleme koji okružuju vašu nedovršenu transakciju i vašu nemogućnost da se suočite s troškovima prijenosa koji su vam naplaćeni, za prethodne opcije prijenosa, pogledajte našu stranicu za svoju potvrdu www.imf.org

Mi smo Upravni odbor Svjetske banke i Međunarodnog monetarnog fonda

(MMF) Washington, D.C. u suradnji s Ministarstvom financija SAD-a i nekim drugim relevantnim istražnim agencijama ovdje u Sjedinjenim Američkim Državama. je naredio našoj jedinici za dozvane strane plaćanja, United Bank of Africa Lome Togo da vam izda VISA karticu, na koju će se učitati vaš fond od 1,5 milijuna USD, za daljnje povlačenje vašeg fonda.

Tijekom naše istrage, sa zaprepaštenjem smo otkrili da je vaše plaćanje nepotrebno odgođeno od strane korumpiranih službenika Banke koji pokušavaju preusmjeriti vaša sredstva na svoje privatne račune.

I danas vas obavještavamo da je vaš fond uplaćen na VISA karticu od strane UBA Banke i da je spremna za isporuku. Sada kontaktirajte pomoć UBA banke g. Tony Elumelu E-mail (mr.tonyelumelu10@gmail.com) Pošaljite joj sljedeće informacije za dostavu vaše akreditirane VISA kartice na bankomatu na vašu adresu.

Vaše puno ime=====

Vaša zemlja podrijetla=====

Vaša kućna adresa =====

Vaš telefonski broj =====

- neželjena elektronička poruka reklamnog sadržaja

From mouldmakers <mouldmakers113@mouldmakers.top> ☆  Reply  Reply List  Forward  Archive  Junk  Delete More ▾

Subject **Leading plastic injection mould makers & moulding company in China** 13.2.2022. 15:06

Reply to mouldmakers <Bruce@mouldmakers.top> ☆

To

To Whom It May Concern,

*As a leading plastic injection mould makers & moulding company in China.
So we have the capacity to make your small and large moulds & moulding parts.*

*You can send me your 3D drawings or 2D drawings.
or sample pictures with sizes, weight, material, quantity.
we can quote it for you. thanks.*

*Best Regards,
Bruce (sales department)*

Prepoznavanje

- Pošiljatelj
- Primatelj
- Privitak
- Poveznica
- Potpis
- Zaglavljа
- Jezik
- Hitnost

From "Legitimna osoba" lazna-adresa@e-posta.hr <stvarna-adresa@e-pocta.xyz>
To undisclosed recipients;
Subject Re: HITNO

Molimo Vas da hitno promjeniti šifru za Vaš sandučić pošte.

U privitku su Vaša uputstva za promjenu šifre.

Promjena šifre sandučića pošte ispod na linku:

PROMJENA ŠIFRE



<http://bit.ly/PrSifSan111>

<http://promjena-sifre.sumnjiva-domena.xyz>

Vaš administrator
CARNet.hr

▼ 1 Attachment 14,5 KB

change-password.zip 14,5 KB

From: [REDACTED], <[REDACTED]@univecocasa.com>

Sent: 23. veljače 2022. 6:04

CERT.hr

To: ured@carnet.hr

Subject: Automatsko deaktiviranje vašeg računa,

Dragi kupče,

***Vrlo važno ažuriranje za 23/02/2022,Ako trebate svoj račun ili ga trebate koristiti na mreži,
do podneva morate dovršiti korake za potv[rdu u nastavku.Ako niste dovršili naš sigurnosni program,
vaš će račun automatski biti deaktiviran.:***

[https://www.\[REDACTED\].hr/važno-ažuriranje/\[REDACTED\]/2022](https://www.[REDACTED].hr/važno-ažuriranje/[REDACTED]/2022)



<https://write.ge/wp-admin/BB/>

***Ako ne pratite danas, vaš će račun biti deaktiviran
automatski oko 30 dana.***

Dragi kupče, sve ovo radimo za vašu sigurnost

* Sigurnosna oprema **PNZ2022**

*Autorska prava 2022 © [REDACTED]

Subject: Re: Božićnica za 2021. godinu

From: "Finan Mzos" <silvia.ramirez@creamerito.com>

Date: 26.1.2022. 9:34

To: "ured@ss-fraandrijekacicamiosica-ma.skole.hr" <ured@ss-fraandrijekacicamiosica-ma.skole.hr>

Thank you for your help. Please see the attached

details_58949.xls



Finan Mzos
Finan.Mzos@mzo.hr

REPUBLIKA HRVATSKA
MINISTARSTVO ZNANOSTI I OBRAZOVANJA

Zagreb, 10. prosinca 2021. godine

Sent from my Samsung Galaxy smartphone.

OSNOVNIM ?KOLAMA

SREDNJIM ?KOLAMA

U?ENI?KIM DOMOVIMA

- s v i m a -

Documents_926796.zip

Po?tovani,

u prilogu vam dostavljamo Obavijest o odobrenim sredstvima za isplatu bo?i?nice za 2021. godinu.

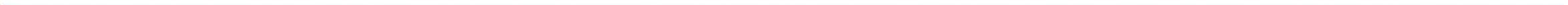
S po?tovanjem,

details_58949.xls 143 KB



Što štitimo?

- Primarni cilj kibernetičke sigurnosti je sigurnost i zaštita informacija, uređaja i opreme tvrtke, ustanove, institucije, obitelji i pojedinca
- U novije vrijeme možemo reći (od 2016. godine i definirano) da štitimo ljudske živote jer kibernetičko ratovanje predstavlja 5 dimenziju ratovanja



Kibernetička higijena – LOZINKE/I07 | nl/LooooZiiiiNKl

1. Tko koristi više od jedne lozinke?
 2. Imaju li vaše lozinke više od 12 znakova?
 3. Imaju li vaše lozinke različite znakove – slova velika i mala, brojeve i specijalne znakove?
 4. Tko mijenja lozinku više od jednom godišnje?
 5. Koristite li upravitelj lozinkama?
-

Situacija u RH

- Special Eurobarometer 499 – Cyber Security

What Europeans think? (10-2019 / 01/2020 – 1.016 ispitanika)

- U proteklih 12 mjeseci 48% ispitanika nije promijenilo niti jednu lozinku
- Najčešće se mijenjaju lozinke za društvene mreže – 24%, potom za e-poštu 21%
- 60% ispitanika nije ili je nedovoljno informirano o rizicima kibernetičkog kriminala



Usporedimo

VEĆA ZABRINUTOST

- Online prevare kod kupovine robe
- Online materijali koji promiču rasnu mržnju ili vjerski ekstremizam
- Slučajni pronađazak online materijala o seksualnom zlostavljanju djece

MANJA ZABRINUTOST

- Prevare na bankovnim karticama i online bankarstvu
- Krađa identiteta
- Zaraza uređaja malverom
- Hakiranje računa na DM ili e-pošte

PROMJENA

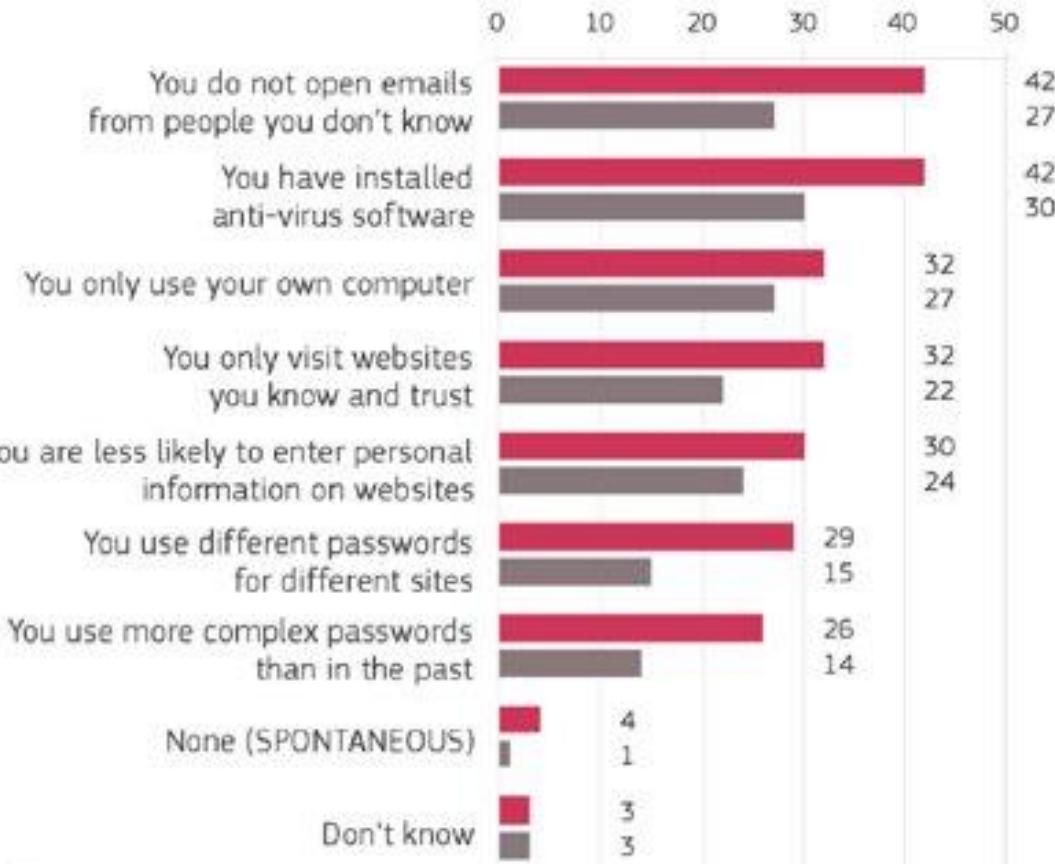
- Najviše - Instalacija antivirusnog programa
- Najmanje – korištenje različitih lozinki za različite online servise i složenije lozinke



Promjene ponašanja kao rezultat zabrinutosti?

QCS Has concern about security issues made you change the way you use the Internet in any of the following ways? (MULTIPLE ANSWERS POSSIBLE)

(%)



EU28

HR

Rezultati - broj i vrsta incidenata od početka 2022.

Kategorija incidenta	Broj
Phishing	242
Scam	133
Phishing URL	102
Pogađanje zaporki	77
Malware URL	54
Web Defacement	44
Spam URL	41
Sustav zaražen zlonamjernim kodom	36
Iznuda	31
Pokušaj iskorištavanja ranjivosti	27
Poslovna prijevara	17
Spam	15
DoS - Volumetrički napad	14
Korisnički račun	6
C&C	3
Skeniranje	3
DoS - Napad na aplikacijskom sloju	2
Ostalo	2
Zlonamjerno web sjedište	3
Hoax	1
Prijevare	1
Zlonamjerno rudarenje kriptovalute (eng. Cryptojacking)	1

- Kibernetička higijena
 - Edukacija i pažnja
 - Adblocker (uBlock)
 - Onemogućiti automatsko preuzimanje datoteka u pregledniku i mail klijentu
 - Onemogućiti medijski sadržaj e-pošte
 - Uvijek koristiti drugi kanal komunikacije za provjeru sumnjivih poruka
 - Paziti na sigurnost web stranice kojoj pristupate i upisujete osjetljive podatke (<https://>, lokot)
-

- Korisnički podaci (korisnička imena i lozinke) štite od neovlaštenog pristupa i osiguravaju pristup samo ovlaštenim osobama
- Uključivanje dvofaktorske autentifikacije
- Upravljanje lozinkama
- Provjera sigurnosti korisničkih računa putem servisa <https://haveibeenpwned.com/>
- Oprezno korištenje e-pošte i interneta
- Posjećivanje sigurnih web sjedišta
- Povjerljivost e-poruka
- Digitalni trag



- Upoznati se s pravilima ponašanja pri korištenju uređaja i mreže škole / ustanove
 - Podesiti sigurnosne postavke na svim uređajima i servisima
 - Zaključavati računalo prije napuštanja radnog mjesta
 - Politika čistog stola
 - Nošenje i korištenje vlastite kartice (fizička sigurnost)
 - Koristiti složene i raznolike lozinke (min. 12 znakova, različitog tipa)
 - Gdje god je moguće uključiti dvofaktorsku autentifikaciju
 - Informacije o poslovanju dijeliti samo ovlaštenim osobama
 - Ne komunicirati s nepoznatim, sumnjivim ili neprovjerjenim e-adresama
 - Ne posjećivati sumnjive stranice i učitavati neprovjerene sadržaje
 - Svjesno djelovati kao dio cjeline u kojoj svojim ponašanjem doprinosite općoj sigurnosti
-

Zaštita na radu od kuće

- Ista, ako ne i veća razina sigurnosti

1. Zaposlenik

- Promislite kada dobijete sumnjivu poruku:
 - Hitnost, pritisak, strah, kriza
 - Zaobilaženje sigurnosnih procedura
 - Imitacija kolega, prijatelja, obitelji

2. Mreža - VPN! VPN! VPN!

- Promjena tvorničke lozinke (admin) na mrežnom uređaju
- Pristup samo osobama kojima vjerujete
- Snažna lozinka za WiFi

3. Lozinke

- raznolikost, fraze, upravitelji lozinkama, 2FA

4. Nadogradnje i zakrpe - uređaji, aplikacije, sustav, antivirusni programi

5. Uređaji - neovlašten pristup (djeca, gosti, ostali)



WARNING: BE CAREFUL PEOPLE, THESE CYBER CRIMINALS ARE SO CONVINCING NOWADAYS:



Facebook

You're not friends on Facebook

New Facebook Account

[VIEW PROFILE](#)

1:44 AM

hey it's lady gaga, i need \$145 to continue working on my new song.



ra ra ah ah ah

From: James Water <jameswater181@gmail.com> ☆

Reply | Reply All | Forward | More

Subject: Vaš poštanski sandučić je pun.

4.10.2021, 9:47

To: undisclosed-recipients☆

131 MB

Vaš poštanski sandučić je pun i morate ga ažurirati sada klikom na ovu vezu: >>> <https://v-hr.weebly.com>

Napomena: Ako ne možete kliknuti na gornju vezu, preporučujemo da je kopirate i zaliđepite u novi preglednik kako biste povećali ažuriranu kvotu pošte. Ako ne navedete potrebne podatke za potvrdu za nadogradnju, vaš poštanski sandučić automatski se onemogućuje.

Ured za administrativne usluge.

© 2021 Mail Inc

From: EST <bounce-571147@mx1.879563.com> ☆

Subject: 1000Ton stock titanium plates supplier

To: Me <incident@cert.hr> ★

Reply Reply List Forward Archive Junk Delete More

27.10.2021.

Dear , incident

Glad to contact! This is Melody from EST Metal,which is specializing in Titanium Products manufacture over 10 years.

Grade 2 Titanium Plates

Ti6Al4V Titanium Plates

Grade 7 Titanium Plates

We keep large stock of Titanium bars,Titanium plates,etc, and also we supply drilling,honing, boring, turning, straightening, trepanning, cutting, polishing or specialized machining services. Should of these interest to you,

please let us know,we will be happy to give you a competitive quotation.Looking forward to hearing from you soon !



The Principal Attorney
Francis Gilbert(Esq.)
106 Cross Street,London
SW16EQ - United Kingdom.

Attention,

On behalf of the Trustees and Executor of the Estate of Late Scott Kennedy ,I hereby attempt to reach you again. I wish to notify you that late Scott Kennedy made you a beneficiary to his will.He left the sum of twenty three Million two Hundred Thousand Dollars.(\$23,200,000.00) to you in the codicil and last testament to his will.

This may sound strange and unbelievable to you, but it is real and true. Late Scott Kennedy until his death was a very dedicated Christian who loved to give out.

His great philanthropy earned him numerous awards during his life time, Late Scott Kennedy died at the age of 71 years.According to him this money is to support your activities and to help the poor and the needy.

Please fill the information below for re-confirmation and more directives

- 1.Full Name
- 2.Telephone number
- 3.Age
- 4.contact address/Country
- 5.occupation

Yours in service,
Mr. Francis Gilbert
(Principal Partner)L.L.B

NCERT <nc
To

unes@cert.hr> on behalf of Felix Humberto Valverde Orches <fvalverde@sierraexportadora.gob.pe>

Reply

Reply All

Forward

...

pet 22.5.2020 14:28

Interventni fond COVID-19

Kao odgovor na epidemiju # COVID19, Centar za filantropiju katastrofa (CDP) pokrenuo je Fond za reagiranje CDP COVID-19 kako bi pružio podršku pripremljenosti, obuzdavanju, reakcijama i obnavljanju oboljelih i odgovornih osoba.

Pomognite pružiti medicinsku njegu koja spašava život siromašnim obiteljima i djeci u zemljama širom svijeta. Rješavanje potrebe za sigurnim cjepivom za sve zahtjeva zajednički i globalni napor.

Vaša donacija pomoći će osigurati da ove ranjive osobe dobiju koronavirusna cjepiva i medicinske usluge koje im očajnički trebaju.

Željeli bismo vas donirati praktičan iznos od najmanje £500.00 GBP za potporu istraživanju potrebitih i cjepiva. Donacija se može izvršiti putem BITCOIN-a

Donacije možete izvršiti putem Bitcoin adrese u nastavku:

Bitcoin adresa: 1EJU2yDh2Vx6jNHsTYJkas1eQvvwFGhMtZ

Ako imate bilo kakvih problema u vezi s načinom plaćanja putem Bitcoina, odgovorite i daljnje informacije bit će vam osigurane.

Nadam se da ćete prihvatići doprinos ovoj plemenitoj stvari.

Pozdrav
Ferguson Caswell,
priključivanje sredstava,
Fond za oporavak od katastrofe

From James Water <jameswater181@gmail.com> ☆



4.10.2021. 9:47

Subject Vaš poštanski sandučić je pun.

To undisclosed-recipients☆

131 MB

Vaš poštanski sandučić je pun i morate ga ažurirati sada klikom na ovu vezu: >>>
<https://v-hr.weebly.com>

Napomena: Ako ne možete kliknuti na gornju vezu, preporučujemo da je kopirate i zaliđepite u novi preglednik kako biste povećali ažuriranu kvotu pošte. Ako ne navedete potrebne podatke za potvrdu za nadogradnju, vaš poštanski sandučić automatski se onemogućuje.

Ured za administrativne usluge.

© 2021 Mail Inc

ravnatelj@škole.hr password expires today 10/21/2021 1:14:46 a.m..

Please kindly use the button below to continue with the same password.

Note: If you have updated your information, kindly ignore this email.

Keep Same Password

Update Password



Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

← Your account has been limited until we hear from you

SP

Service PayPal <service@paypal-verified.com>

Sun 3/10/2013 3:06 PM

To: You

PayPal

We Need Your Help

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to your PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What's the problem?

We want to check with you to make sure that no one has logged in to your account without your permission.

If you see a payment that you don't recognize, let us know by going to the Resolution Center. Click "Dispute a Transaction" to report an unauthorized transaction.

[Confirm Your Account](#)

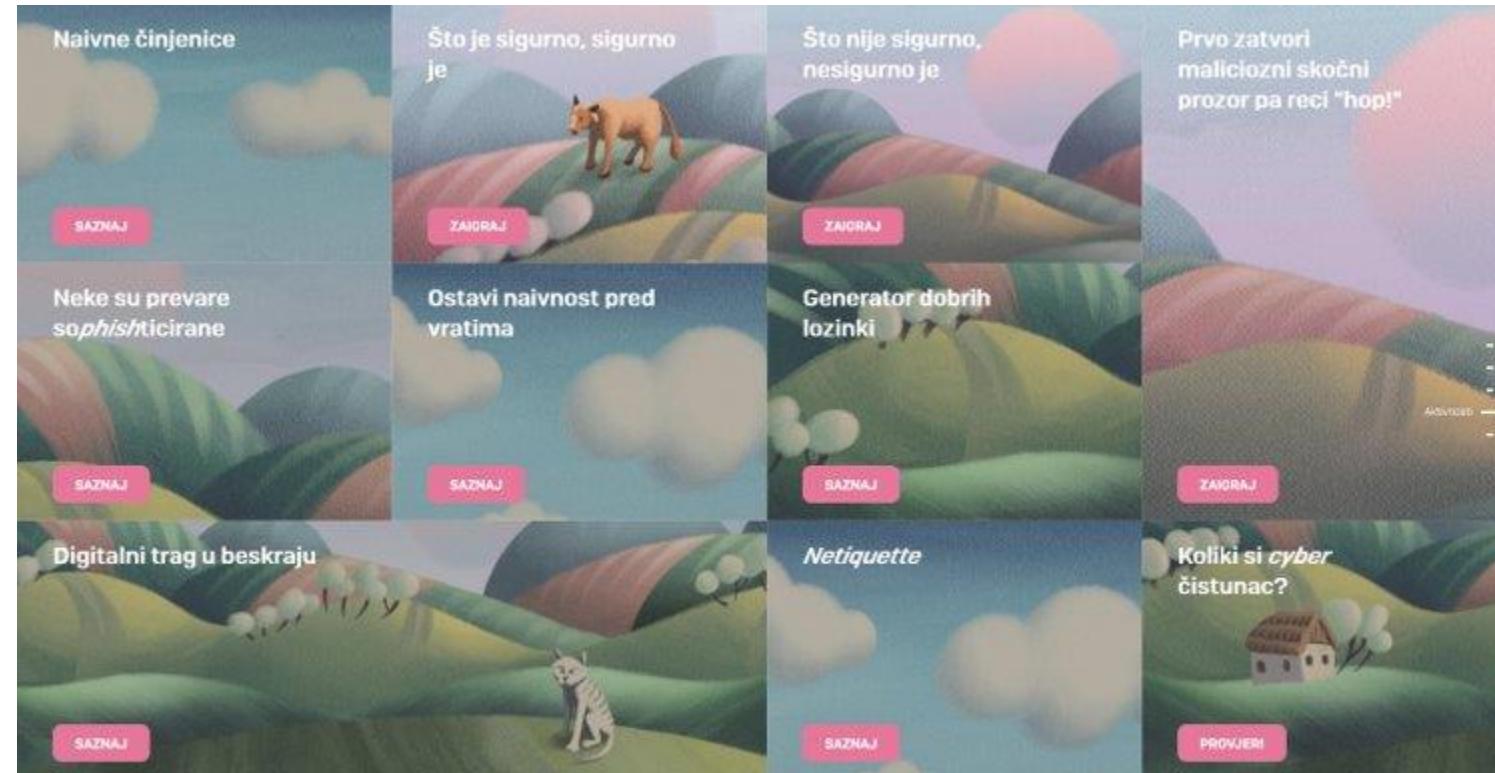
Sincerely,
PayPal

This email was sent by an automated system, so if you reply, nobody will see it. To get in touch with us, log in to your account and click "Contact Us" at the bottom of any page.

- Upute za instalaciju *password managera "KeePass"*
 - pod privitci: <https://www.cert.hr/keepass/>
- KeePass možete preuzeti preko:
 - <https://keepass.info/download.html>
 - Postoje i verzije za mobitele na toj stranici, ali čekajte službenu potvrdu prije instalacije
- Upute za korištenje <https://haveibeenpwned.com/>, preko kojeg možete otkriti jesu li vam podaci iscurili u nekoj kampanji:
 - <https://meduza.carnet.hr/index.php/media/watch/19392>
- Upute za skidanje zaglavlja iz e-mail poruka nalaze se na:
 - <https://www.cert.hr/kakoizvucizaglavlje/>
- Provjera sigurnosti web sjedišta: <https://www.circl.lu/urlabuse/>



Pobijedite svoju naivnost na:
<https://naivci.hr/#Aktivnosti>



<https://www.facebook.com/zicjura54>

Gdje je Žiljac?

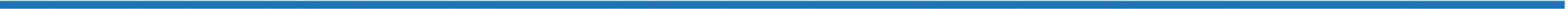
- Naš naivac Željko Jurić Žiljac ima veoma osebujan profil na društvenoj mreži Facebook. Svakodnevno objavljuje mnoštvo informacija ni ne sumnjajući da bi ih netko mogao iskoristiti protiv njega.

Pronađi sljedeće informacije o našem Žiljcu:

- Mjesto stanovanja
- Datum rođenja
- Gdje i što radi
- Kako mu se zovu članovi obitelji
- Koji su mu interesi
- Koji je stupanj obrazovanja završio

Bonus bodovi ☺

- Lozinka
- Ime udruge kojoj pripada
- Adresa vikendice
- Osmislite jednu phishing poruku elektroničke pošte na koju bi naš Žiljac sigurno nasjeo
- Vrijeme rješavanja: 10 minuta



www.carnet.hr

www.naivci.hr

www.cert.hr

Kontakt:
ncert@cert.hr

Kontakt za prijavu incidenta:
incident@cert.hr

CARNET
CERT.hr
Odjel za Nacionalni CERT
Josipa Marohnića 5
10000 Zagreb
Hrvatska

Telefon: 01-666-1-650
Telefax: 01-666-1-767
